

EXAMINER'S AMENDMENT

1. An examiner's amendment to the record appears below. Should the changes and/or additions be unacceptable to applicant, an amendment may be filed as provided by 37 CFR 1.312. To ensure consideration of such an amendment, it MUST be submitted no later than the payment of the issue fee.

Authorization for this examiner's amendment was given in a telephone interview with Don Gibson on 4/9/09.

2. The application has been amended as follows:

Claim 1. (Currently Amended) A system for protecting sensitive information in a network comprising:

a network component for storing the sensitive information necessary for authorized network access; and

a network device, attachable to the network, that lacks the sensitive information necessary for authorized network access and is inoperative, at least in part, until the sensitive information is stored therein;

wherein, when the network device is attached to the network, the sensitive information necessary for authorized network access is downloaded from the network component and stored in the network device so that the network device becomes operational;

wherein, when the network device is disconnected from the network, the sensitive information necessary for authorized network access is erased from the network device, thereby making the network device inoperative at least in part and

removing the sensitive information necessary for authorized network access from the network device;

wherein the network component is located in a secure environment comprising security for both physical access and network communications;

wherein the sensitive information necessary for authorized network access is selected from the group consisting of configuration information, a software image, and a combination of the foregoing; and

wherein the sensitive information is bundled with self-extracting software as stored at the network component.

Claim 2. (Cancelled)

Claim 3. (Currently Amended) The system of claim [[2]] 1, wherein the configuration information is selected from the group consisting of a password, a user ID, a network security key, and any combination of the foregoing.

Claim 8. (Currently Amended) A method for protecting sensitive information in a network comprising:

storing the sensitive information necessary for authorized network access at a network component;

attaching a network device to the network, the network device lacking the sensitive information necessary for authorized network access and being inoperative, at

least in part, until the sensitive information necessary for authorized network access is stored therein;

downloading the sensitive information necessary for authorized network access from the network component to the network device;

storing the sensitive information necessary for authorized network access in the network device so that the network device becomes operational on the network;
~~and~~

when the network device is disconnected from the network, erasing the sensitive information necessary for authorized network access from the network device, thereby rendering the network device inoperative, at least in part;

wherein the network component is located in a secure environment comprising security for both physical access and network communications;

wherein the sensitive information necessary for authorized network access is selected from the group consisting of configuration information, a software image, and a combination of the foregoing; and

wherein the sensitive information is bundled with self-extracting software as stored at the network component.

Claim 9. (Cancelled)

Claim 10. (Currently Amended) The method of claim [[9]] 8, wherein the configuration information is selected from the group consisting of a password, a user ID, a network security key, and any combination of the foregoing.

Claim 15. (Currently Amended) A device that is non-operational on a network unless the device is storing configuration information necessary for authorized network access comprising:

an interface for communicating with the network;

a memory whose contents are erased upon loss of power to the device; ~~and~~
means for downloading from a network component of the network and storing in the memory the configuration information necessary for authorized network access so that the configuration information necessary for authorized network access is not retained when the device is powered down, wherein the configuration information necessary for authorized network access, when stored in the memory, permits the device to operate on the network;

wherein the device is a wireless access point (AP);

wherein the network component is located in a secure environment comprising security for both physical access and network communications;

wherein the means for downloading includes a bootstrap program for downloading from the network an executable image;

wherein the executable image permits the device to download the configuration information necessary for authorized network access;

wherein the configuration information necessary for authorized network access includes security information for allowing end user devices to access the network through the wireless AP; and

wherein the device provides network access to a voice over IP phone that stores the security information and a software image in volatile memory.

Claim 16. (Canceled)

Claim 17. (Canceled)

Claim 18. (Currently Amended) The device of claim [[16]] 15, further comprising means for storing the executable image in the memory.

Claim 19. (Canceled)

Claim 20. (Canceled)

Claim 22. (Currently Amended) A network system, comprising:

a switch for attaching a device to a network so that information can be communicated between the device and the network system, wherein the device is not fully operational when first connected to the switch; and

means for downloading configuration information necessary for authorized network access from a network component of the network system to a volatile memory

included in the device in response to a request from the device, so that the configuration information necessary for authorized network access is not retained in the device when the device is powered down, the device being operable on the network after the configuration information necessary for authorized network access is downloaded into the volatile memory;

means for downloading an executable image from the network system to the device;

wherein the request is generated by running the executable image on the device;

wherein the device is a wireless access point (AP);

wherein the network component is located in a secure environment comprising security for both physical access and network communications;

wherein the configuration information necessary for authorized network access includes security information for allowing end user devices to access the network system through a wireless AP; and

wherein the device provides network access to a voice over IP phone that stores the security information and a software image in volatile memory.

Claim 23. (Canceled)

Claim 24. (Canceled)

Claim 26. (Canceled)

Claims 29-38. (Canceled)

Allowable Subject Matter

3. Claims 1, 3-8, 10-15, 18, 21-22, 25 and 27-28 are allowed.
4. The following is an examiner's statement of reasons for allowance: The present invention is directed to improve network security by limiting the amount and type of information stored at network edge devices, like access points. The independent claims disclose a network component for storing sensitive information and an access point that is not fully operational until it is attached to the network and has downloaded the sensitive information (i.e. software image and configuration information). When downloaded, the sensitive information is stored in the access point so that when the access point is disconnected from the network, the sensitive information is erased, making the device inoperative and removing the sensitive information. When downloaded, the image is necessary for the access point to operate on the network, it generates a request to the network to download configuration information to the access point and permit the access point to become fully operational. The prior arts of record fail to anticipate or render the above limitations obvious.
5. Any comments considered necessary by applicant must be submitted no later than the payment of the issue fee and, to avoid processing delays, should preferably accompany the issue fee. Such submissions should be clearly labeled "Comments on Statement of Reasons for Allowance."

6. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Minh Dieu Nguyen whose telephone number is 571-272-3873.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Gilberto Barron can be reached on 571-272-3799. The fax phone number for the organization where this application or proceeding is assigned is (571) 273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

/Minh Dieu Nguyen/
Primary Examiner, Art Unit 2438